REMARKS/ARGUMENTS

Applicants appreciate the Examiner granting the telephonic interview of April 30, 2010. Enclosed herewith is an interview summary in accordance with M.P.E.P. §703.04.

Applicants further appreciate the Examiner's continued thorough search and examination of the present patent application.

Claim Objections

Claims 31-43 stand objected to on the grounds that these claims are not very specific about the nature of the parameters and the relationship between the parameters. As discussed during the telephone interview of April 30, 2010, the nature of the parameters and the relationship there-between are clearly set forth in claims 31-43. Pursuant to the Examiner's request, claim 35 has been amended to clarify that the value, "Z," represents "a result of a mask operation process and received from the terminal." Therefore, claims 35 and 36-38, which depend directly from claim 35, are similarly clear and specific. Applicant respectfully requests reconsideration.

Claim Rejections

Claims 31-43 stand rejected under 35 U.S.C. §102(e) as being anticipated by Peyravian et al. ("Peyravian," U.S. Patent Application Publication No. 2004/0158708). Applicants respectfully traverse this rejection.

Claims 31-34 and 39-43

Applicants' claim 31, as amended, is directed to a "computer readable storage medium storing an authentication program...for mutual authentication between a terminal and a server." The program allows a computer to execute a "memory process to pre-store an authentication information P for terminal storage, and an RSA public key." The computer is further allowed to execute a "concatenation process to yield a value W" and a "mask operation process to yield a value Z." The value "W" is yielded "using a specific calculation formula with ... P' and a password entered for authentication." The value "Z" is yielded "using a specific calculation formula with ... W, the stored RSA public Key ... and an internally generated random number

T." The value "Z" is sent to the server. Peyravian does not teach, suggest or disclose this combination of features.

In Peyravian, a password, "PW," is a "a secret one-time-use password that is known by the client and a server" (see [0016]), and is assumed to be "sufficiently long" (see paragraph [0013]). Peyravian's password PW needs to be sufficiently long because if it is short enough to be remembered by a user, Peyravian's method would be vulnerable to an attacker performing active attacks, such as eavesdropping, modifying/deleting/replaying messages or the like. Unlike Peyravian, applicants' claimed "W" is not one-time-use value and is yielded using a "password entered for authentication."

Moreover and unlike applicants' claim 31, Peyravian requires that both the client and the server have respective public/private key pairs (see Fig. 1). Applicant's claimed authentication process does not provide the terminal with access to a "public/private key pair while the terminal uses the "RSA public key (N, e)."

Furthermore, applicants' claim 31 value "W" is computed with "authentication information P'" and a "password entered for authentication." Thus, P' is not shared with the server. Peyravian's PW, in contrast, is shared with the server. Peyravian does not teach, disclose or suggest applicants' computed value "W" that is "yielded" using "authentication information P'" and a "password entered for authentication."

Moreover, applicants' claim 31 value "Z" is yielded with the value, "W," the "RSA public key" and a random number, "T." Thus, the value Z is yielded using the hashed value of W and RSA public-key encryption of the random number at the same time. Peyravian, in contrast, generates "ARGc," by hashing a concatenation of a user's ID, a shared (between client and server) password PW, the public key and a random number (see Fig. 1, step 115). Peyravian's client then forms "an extended concatenation using the ID, the previous hashed value and the public-key encryption, in a separate step (see [0010]).

Thus, as set forth above, features of applicants' amended claim 31 are not taught, suggested or disclosed by Peyravian and, accordingly, Peyravian cannot anticipate applicants' claim 31 under 35 U.S.C. §102(e).

Claims 32-34 and 39-43 depend directly or indirectly from claim 31 and are patentable as well as because of the combination of features in those claims with the features set forth in the

claim(s) from which they depend.

Claim 35, as amended, is also patentably distinct from Peyravian. Claim 35 recites a "computer readable storage medium storing an authentication program for mutual authentication" and requires a memory process to "pre-store a password verification data H" for "server registration" and an "RSA private key (N, d)." The Examiner cites Figure 1, 140 for support that Peyravian teaches this feature. Included in 140, however, is Peyravian's password "PW," which as noted above, is shared by "the client and a server" ([0016]). Applicants' password verification data "H" in contrast is not shared between a client and server. Moreover, applicants' claim 35 value, "T," that is yielded using applicants' claim 35 "master key generation process" with the "input of the stored password verification data H, RSA private key (N, d) and a value Z received from the terminal." Thus, the master key generation process results in a single step. Peyravian, in contrast, involves the hashed value and the private-key decryption in separate steps (see Peyravian Figs. 1, 3 and 4). Thus, features of applicants' claim 35 are not taught, suggested or disclosed by Peyravian and, accordingly, Peyravian cannot anticipate applicants' claim 35 under 35 U.S.C. §102(e).

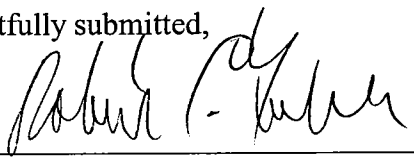
Claims 36-38 depend directly from claim 35, and are patentable as well as because of the combination of features in those claims with the features set forth in claim 35.

Conclusion

Accordingly, and in view of the above-identified amendments to the claims and remarks set forth above, the Examiner is respectfully requested to reconsider the application, allow the claims as amended and pass this case to issue.

THIS CORRESPONDENCE IS BEING SUBMITTED ELECTRONICALLY THROUGH THE PATENT AND TRADEMARK OFFICE EFS FILING SYSTEM ON May 14, 2010.

Respectfully submitted,



Robert C. Faber
Registration No.: 24,322
OSTROLENK FABER LLP
1180 Avenue of the Americas
New York, New York 10036-8403
Telephone: (212) 382-0700

RCF:JJF:ck

{01140631.1}